CI1355 / INFO7056: Tópicos em Algoritmos - Fundamentos da Criptografia 2026

Primeira lista de exercícios

Professor: Nicollas Mocelin Sdroievski

Essa lista de exercícios aborda os assuntos da primeira parte da disciplina de Tópicos em Algoritmos - Fundamentos da Criptografia. Esta lista pode ser realizada por grupos de até três alunos, e deve ser entregue (em formato manuscrito ou formatada com LaTeX) por um dos membros até às 23:59 do dia 22/09. A entrega pode ser feita por e-mail (*nmsdroievski[arroba]ufpr.br*) ou presencialmente durante o horário de aula.

Exercícios para entrega

Todos os exercícios possuem o mesmo peso para fins de avaliação.

1. **(Exercício 2.9 do livro, adaptado).** Neste exercício, exploramos diferentes condições em que as cifras de César, mono-alfabética e de Vigenère são perfeitamente secretas:

   (a) Prove que se apenas um caractere é cifrado, então a cifra de César é perfeitamente secreta.

   (b) A cifra mono-alfabética é perfeitamente secreta para mensagens com dois caracteres? Justifique sua resposta.

   (c) Prove que a cifra de Vigenère usando período fixo t é perfeitamente secreta quando usada para cifrar mensagens de tamanho t.

2. Para cada função abaixo, indique se a função é negligenciável ou não, e justifique sua resposta:

   (a) $f(n) = 2^{-n/2}$.

   (b) $f(n) = n^{-100}$.

   (c) $f(n) = 2^{-\log^3 n}$.

3. **(Exercício 3.6 do livro, adaptado).** Seja G um gerador pseudoaleatório com fator de expansão $\ell(n) > 2n$. Para cada construção abaixo, indique se a construção é ou não um gerador pseudoaleatório, e justifique sua resposta. A seguir, $||$ denota concatenação e $\overline{x}$ denota o complemento da string x, onde cada bit é trocado pelo bit oposto.

   (a) $G_1(s) \doteq G(s)||\overline{G(s)}$, onde $s \in \{0,1\}^n$.

   (b) $G_2(s_1, \ldots, s_n, s_{n+1}, \ldots, s_{2n}) \doteq G(s_1, \ldots, s_n)$.

   (c) $G_3(s) \doteq G(0^n||s)$, onde $s \in \{0,1\}^n$.[1]

4. Neste exercício, vamos mostrar que, em uma cifra Π que é CPA-segura, nenhum adversário eficiente $\mathcal{A}$ consegue recuperar sequer um bit de uma mensagem criptografada com Π com vantagem não-negligenciável.

   Seja $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ uma cifra de chave privada onde $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$ e $\mathcal{A}$ um adversário. Considere o seguinte experimento $\mathsf{PrivK}^{\mathsf{cpa\text{-}1}}_{A,\Pi}(n, i)$:

[1] Dica: use G_2 na sua justificativa.

- O desafiante gera uma chave k ao executar $\mathsf{Gen}(1^n)$.
- O adversário $\mathcal{A}$ recebe como entrada 1^n e acesso de oráculo à $\mathsf{Enc}_k(\cdot)$.
- O desafiante amostra $m \leftarrow \{0,1\}^n$ de maneira uniforme, computa $c \leftarrow \mathsf{Enc}_k(m)$ e envia c para $\mathcal{A}$.
- O adversário continua a ter acesso de oráculo para $\mathsf{Enc}_k(\cdot)$, e produz um bit b_i.

Definimos $\mathsf{PrivK}^{\mathsf{cpa\text{-}1}}_{A,\Pi}(n,i) = 1$ se, no fim da execução, $b_i = m_i$, isto é, se o adversário acerta o valor do i-ésimo bit da mensagem m cifrada pelo desafiante.

Prove que, se Π é uma cifra CPA-segura, então vale que, para todo algoritmo probabilístico polinomial $\mathcal{A}$ e $i \in \{1,2,\ldots,n\}$, existe uma função negligenciável negl tal que para todo n:

$$\Pr\left[\mathsf{PrivK}^{\mathsf{cpa\text{-}1}}_{A,\Pi}(n,i) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n),$$

onde a probabilidade é sobre a aleatoriedade do desafiante (para amostrar k e também a mensagem m) e a aleatoriedade de $\mathcal{A}$.

5. Seja $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ uma função pseudoaleatória (chaveada). Neste exercício, vamos mostrar que nenhum adversário probabilístico polinomial $\mathcal{A}$ consegue encontrar dois valores x e y tal que $F_k(x) = F_k(y)$ com probabilidade não-negligenciável.

   (a) Seja $\mathcal{A}$ um algoritmo de tempo polinomial $q(n)$ tal que $\mathcal{A}^{\mathcal{O}(\cdot)}(1^n) = 1$ se e somente se $\mathcal{A}$ encontra uma colisão na função $\mathcal{O} : \{0,1\}^n \to \{0,1\}^n$. Usando o Lema A.15 do livro, argumente que, se $f : \{0,1\}^n \to \{0,1\}^n$ é uma função aleatória, então: [2]

   $$\Pr\left[\mathcal{A}^{f(\cdot)}(1^n) = 1\right] \leq \frac{q(n)^2}{2^{n+1}}.$$

   (b) Usando o fato de que F é pseudoaleatória, conclua que existe uma função negligenciável negl tal que

   $$\Pr\left[\mathcal{A}^{F(\cdot)}(1^n) = 1\right] \leq \mathsf{negl}(n).$$

Exercícios para pós-graduação

6. **(Exercício 3.7 do livro, adaptado)**. Prove que, se G não é um gerador pseudoaleatório, então a construção 3.17 (da aula 7) não é EAV-segura.

7. **(Exercício 2.8 do livro, adaptado)**.

   (a) Modifique o experimento $\mathsf{PrivK}^{\mathsf{mult}}_{A,\Pi}(n)$ de maneira a capturar uma noção de indistinguibilidade para múltiplas mensagens *distintas*. Isto é, o esquema não precisa ser seguro caso a mesma mensagem seja cifrada duas ou mais vezes.

   (b) Considere a seguinte cifra simétrica $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ para espaço de mensagens $\{0,1\}^n$ baseada em uma permutação pseudoaleatória/cifra de bloco F:

[2] Dica: como f é aleatória, a única maneira que $\mathcal{A}$ pode tentar extrair informação de f é através de consultas. Qual o máximo de consultas que $\mathcal{A}$ consegue realizar?

- $\mathsf{Gen}(1^n)$ retorna uma chave k para F.
- $\mathsf{Enc}_k(m) = F_k(m)$.
- $\mathsf{Dec}_k(c) = F_k^{-1}(c)$.

Mostre que Π respeita à sua definição de segurança do item anterior.

Exercícios opcionais

8. Recupere as seguintes mensagens a partir do texto cifrado:[3]

   (a) O seguinte texto cifrado, produzido a partir de uma cifra de César e uma mensagem original em português:

   ```
   JXENWLNMXAJBKJCJCJBNBCNYARWLRYRXZDNYJANLNEDUPJACNVDVJPAJWMNBRPWR
   ORLJLJXORUXBXORLJNJUNRMJERMJXBOXACNBNBVJPJVXBOAJLXBXBONURINBMNEX
   AJVXBCARBCNBXBYADMNWCNBUDMRKARJVXBRWPWDXBNJBBRVLJVRWQJJQDVJWRMJM
   N
   ```

   (b) O seguinte texto cifrado, produzido a partir de uma cifra de Vigenère com tamanho de chave entre 2 e 10 e uma mensagem original em português:

   ```
   UDGTJXTVEMQFIMQJYNVKEPQGEXOXJJETGJNTVXSNIJPLIRQJYNCFSAVXHJSNMUQX
   QZWXELTXHRVHRJQFILCEIJCEQJPXQJHTPJRHVZWXEVGMEMGWIVKFIXSNINWZVRVH
   QJUTSDVKEVGMEMGXGJNFELNTVJSNIJONWRETUDGXWLWMSJQESWIXWNLTPRPWEJKG
   HJSNIJOTVPWKEZWXEVWELNTJYNGNEVQLISCTQJFTQNUFSJHTWCCWEYQKUDGTQNVT
   HNFXQROXTJTMMMCFEBCHYCTTQNVTHNGLEDFTHNEEEACJYNCLTJNTZACLUDGXYOCE
   SWCHWNLTQJTFEMCLGXOHTAGVIWGFEATTWCCWEBEHQOGKZXTTTNPTWPWTVMCWEBPT
   EUOTVJTTTXTJYNCFICCWIMGFMVGHUDGXYLNTQXOTWJQNXACFICCWINCIEISNIJOT
   VACJYNCOSWVTHNFXMAGFFXTTWNVKEWUYSAOXRJETPVCVPJTTIZWXEJPLMJSNIVGT
   VACLXJCVEAPXWNLTYVFBEJRTKJFTTXTJYNCFICCWIMGFMVGHUDGIIWUHQJUTSDVK
   EVGMEMGXGQCFELNTVJSNIXOXHXFTWXNBHJQLIJHTWCGXUDGHEKTTGXEHQRIHQNUF
   SBGMSAPXEXOXRXUTGNKMEEGEUDGHIBRXPQQMVJITRJHTGNWFFACGHXTTWCTHHNCE
   IPTBEYCLWJFTTXTJYNCFICCWIMGFMVGEIVDKEWETEXWMVJOXXJFXIJNFELNTVJSN
   IWCHWNLTTAGVMBQFERUWSZWXYVCTPNIKMJRTVJCJYRGMEACTPVCTJUKMENSNIXVX
   YBKEIWEBSVGTFACVILCWEMKTTXTJYNCFICCWIMGFMVGTFAKZSVCLEXWMVJOXXJFX
   ILCGWJEHHJETQRPAEMCJYNCTVCGFIJDKEJGLXACWEVGLQXSNIWCWEBCBFJGJYNPB
   RPWXQJCMVJRTPQGISASNIJOXXJFXHNOBQNREECGBENCHYCTTQNVTHNGVEWETSACK
   ENSNIJOBRQCESDENVJUXNJCFTJTTHJRHVZWXEVGMEMGWIVKFIJOHVNCHYCTTQNVT
   HNVTQKGFILJTQJEEEAC
   ```

9. Prove que a máquina Enigma não constitui uma cifra perfeitamente secreta, mesmo quando usada para criptografar apenas uma letra.

10. Prove a seguinte implicação do Lema 2.6 da aula 4: Se uma cifra não é perfeitamente secreta, então também não é perfeitamente indistinguível. [4]

11. Prove que o one-time pad não é IND-CPA seguro.

[3] Confira o material do grupo de estudos ministrado na UNESPAR para dicas.

[4] Dica: construa um adversário para o experimento e analise sua probabilidade de sucesso condicionada no valor do bit b amostrado pelo desafiante.

12. Prove que se existe uma função unidirecional, então $\mathsf{P} \neq \mathsf{NP}$.[5]

13. Prove que, se existe um gerador pseudoaleatório com fator de expansão $\ell(n) = 2n$, então existe uma função unidirecional.

14. **Desafio.** Seja $\mathsf{negl}_1, \mathsf{negl}_2, \ldots$ uma sequência de funções negligenciáveis e seja $p(n)$ um polinômio em n. Prove que $f(n) = \sum_{i=1}^{p(n)} \mathsf{negl}_i(n)$ não necessariamente é uma função negligenciável.

15. **Desafio. (Exercício 3.29 do livro, adaptado)** Sejam $\Pi_1 = (\mathsf{Enc}_1, \mathsf{Dec}_1)$ e $\Pi_2 = (\mathsf{Enc}_2, \mathsf{Dec}_2)$ duas cifras simétricas tal que pelo menos uma das duas é CPA-segura (mas você não sabe qual). Mostre como construir uma cifra Π que é garantidamente CPA-segura contanto que pelo menos uma dentre Π_1 e Π_2 seja CPA-segura.[6]

[5] Dica: prove que se $\mathsf{P} = \mathsf{NP}$, então não existem funções unidirecionais

[6] Dica: a partir da mensagem original, construa duas mensagens tal que conhecimento de apenas uma não revela nada sobre a mensagem original, porém conhecimento das duas permite recuperar a mensagem original.